# Sentinel 7.3.1 Release Notes

July 2015




Sentinel 7.3.1 includes new features, improves usability, and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Sentinel forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Sentinel NetIQ Documentation page. To download this product, see the Sentinel Product Upgrade website.



## 1 What’s New?

The following sections outline the key features and software issues resolved in this release:



### 1.1 Java 8 Upgrade

Sentinel 7.3.1 includes Server Java Runtime Environment (JRE) version 8 update 45, that includes fixes for several security vulnerabilities and also improves Sentinel performance.

To be able to launch Sentinel Control Center and Solution Designer on any client computer, you must install JRE 8 on the client computer.

The JRE folder structure has been changed from `/opt/novell/sentinel/jre` to `/opt/novell/sentinel/jdk/jre`.

**NOTE:** Sentinel 7.3 documentation does not reflect the changes to the JRE folder structure.

## 1.2 Security Vulnerability Fixes

This service pack resolves the following security vulnerabilities:

- Logjam (CVE -2015-4000)
- Bar Mitzvah (CVE-2015-2808)

---

**NOTE**

- As part of fixing these security vulnerabilities, there are some changes to the communication protocols used on the Sentinel server. Therefore, when you upgrade the Sentinel server to version 7.3.1, you must also upgrade the Collector Manager, Correlation Engine, and the NetFlow Collector Manager to version 7.3.1 for seamless communication.
- Fixing these vulnerabilities in Sentinel has caused communication failure with Change Guardian and Secure Configuration Manager. For more information about the workaround for this issue, see Section 4.4, "Cannot Receive Events from Secure Configuration Manager After Upgrading to Sentinel 7.3.1," on page 14 and Section 4.5, "Cannot Receive Events from Change Guardian After Upgrading to Sentinel 7.3.1," on page 14.

---

## 1.3 Software Fixes

Sentinel 7.3.1 includes the following software fixes that resolve several previous issues.

For the list of software fixes and enhancements in previous releases, see the specific release notes.

### 1.3.1 Cannot Launch Sentinel Control Center and Solution Designer Using JRE 8 When Sentinel is in FIPS 140-2 Mode

**Issue:** When the Sentinel server is running in FIPS 140-2 mode, you cannot launch Sentinel Control Center and Solution Designer in the client computer using Java Web Start if the JRE version is 8 or later. `(BUG 907263)`

**Fix:** Sentinel 7.3.1 supports JRE 8. You can now launch Sentinel Control Center and Solution Designer when Sentinel is in FIPS 140-2 mode.

### 1.3.2 Occurrences Count Decreases After Refreshing the Alert View

**Issue:** In the alert view, the **Occurrences** count decreases when you refresh the alert view. `(BUG 913838)`

**Fix:** Few minutes after the alert roll up happens, **Occurrences** count displays the correct value when you refresh the alert view.

### 1.3.3 Alert Roll-up Occasionally Fails and Sentinel Incorrectly Creates New Alerts

**Issue:** Sentinel might create a new alert instead of rolling up alert information to an existing alert. This is a sporadic issue. `(BUG 914512)`

**Fix:** Sentinel does not create new alerts when the alert information can be rolled up to an existing identical alert.

### 1.3.4 Sentinel Does Not Display Trigger Events for Remote Alerts

**Issue:** In alert views, when you click **View Details** next to any remote alert and go to the Alert Details page, trigger events for that alert do not display in the **Associated Data** panel. `(BUG 916116)`

**Fix:** You can view the trigger events for remote alerts in the Alert Details page.

### 1.3.5 Sentinel Does Not Display Customized Alert Properties for Remote Alerts

**Issue:** The **State** and **Priority** fields in remote alerts do not display any data if they are customized. `(BUG 915762)`

**Fix:** Sentinel 7.3.1 improves the mechanism to communicate with the remote data source server to obtain customized values. Sentinel now displays data for **State** and **Priority** fields correctly.

### 1.3.6 Sometimes Sentinel Does Not Display Alerts in Alert Views After a Restart

**Issue:** Sometimes, Sentinel does not display alerts in alert views if you restart Sentinel. `(BUG 916133)`

**Fix:** Alert views display alerts correctly even after you restart Sentinel.

### 1.3.7 Documentation for Methods Related to Sentinel Plug-ins Requires Updating

**Issue:** The documentation for some operations in Sentinel Plug-ins does not provide examples about how to use the Sentinel Plug-ins REST APIs. `(BUG 744255)`

**Fix:** Sentinel API documentation contains examples about how to use REST APIs for performing various operations.

### 1.3.8 SpyEye Tracker Feeds Have Been Discontinued by its Provider

**Issue:** The data provider for the SpyEye Tracker feed has discontinued updates to this feed, stating that the SpyEye threat appears to be mitigated. This feed plug-in is still bundled in Sentinel. The data provider no longer supplies valid threat feeds; so, the feed plug-in populates the dynamic lists with unexpected data, and related correlation rules do not work properly. The Feeds user interface only indicates that data was processed successfully, but does not indicate that the data is invalid. `(BUG 916560)`.

**Fix:** Go to the Solution Manager and upgrade the Threat Intelligence Solution Pack version to 2011.1r2. This solution pack removes SpyEye Tracker components. For more information, see the Threat Intelligence Solution Pack documentation on the Sentinel Plug-ins website.

### 1.3.9 Sentinel Web Interface Might Not Launch in FIPS 140-2 Mode

**Issue:** If Sentinel is in FIPS 140-2 mode, the Sentinel Web interface does not launch in Internet Explorer (with TLS version set only to 1.2) and logs an exception in the server logs. In Chrome, the Sentinel Web interface launches but logs an exception. `(BUG 926093)`

**Fix:** You can now launch the Sentinel Web interface in Internet Explorer and Chrome without logging any exceptions when Sentinel is in FIPS 140-2 mode.

### 1.3.10 Launching the Sentinel Web Interface with Port Forwarding or Destination Network Address Translation Displays a Blank Page

**Issue:** When you launch the Sentinel Web interface using port forwarding or Destination Network Address Translation (DNAT), Sentinel Web interface displays a blank page. `(BUG 694732)`

**Fix:** Sentinel Web interface launches correctly. The URL built when you use port forwarding or DNAT will not have any port number.

### 1.3.11 Sentinel Might Display an Error When You Create or Regenerate a Baseline

**Issue:** When you create or regenerate a Security Intelligence baseline, Sentinel creates the baseline successfully, but displays an error message. `(BUG 848067)`

**Fix:** Sentinel creates Security Intelligence baseline correctly, and does not display any error message.

### 1.3.12 Security Intelligence Dashboards Consume Large Amounts of Memory

**Issue:** Security Intelligence (SI) dashboards consume large amounts of memory, which results in the Sentinel server shutting down. `(BUG 906615)`

**Fix:** Sentinel 7.3.1 fixes this issue by improving the SI processing mechanism.

### 1.3.13 Cannot Set Action Time Attributes When Creating Correlation Rules in Some Languages

**Issue:** If you have set your system language to a language other than English, such as German and Australian English, the Action Time attributes do not work while creating expressions for a new correlation rule. `(BUG 888663)`

**Fix:** Sentinel now reads the browser settings made for the selected system language, and accordingly maps the internal parameters created for the Action Time attributes. Now you can use Action Time attributes in any language, while creating expressions for a new correlation rule.

### 1.3.14 Search Filters Do Not Work in Distributed Reports

**Issue:** When you run a distributed report, Sentinel does not apply the search filters, such as the security filter for the role. All the events are recorded in the report. `(BUG 915179)`

**Fix:** When running distributed reports, Sentinel applies the role security filter of the user who runs or schedules the distributed report.

### 1.3.15 Event Source Sorting Does Not Work Correctly

**Issue:** When you sort the event sources for Create Date, Parse, or EPS columns in the **Collection** > **Event Sources** tab, sorting does not work correctly. `(BUG 899652)`

**Fix:** In Sentinel 7.3.1, sorting of event sources works correctly.

### 1.3.16 Sentinel Does Not Display Values for Long Data Type Event Fields

**Issue:** If event fields are of long data type, and if the value is longer than `[-9007199254740991 TO 9007199254740991]`, Sentinel does not display any value for those fields. `(BUG 911147)`

**Fix:** Sentinel displays long data type event fields correctly. If the event fields are of long data type and if the value is longer than `[-9007199254740991 TO 9007199254740991]`, Sentinel treats those fields as text strings.

### 1.3.17 Sentinel Generates Duplicate Audit Events for User Logins

**Issue:** When users log in to the Sentinel Web interface, the Sentinel server authenticates them twice. This results in generation of duplicate audit events for user logins. `(BUG 891602)`

**Fix:** Sentinel server does not generate duplicate audit events for user logins.

### 1.3.18 Sentinel Server Might Not Restart Correctly If There Are Large Number of Connections to the PostgreSQL Database

**Issue:** When you restart the Sentinel server, it might not start correctly if there are large number of connections to the PostgreSQL database, resulting in huge memory utilization. `(BUG 923365)`

**Fix:** The PostgreSQL database uses a fixed size pool, which reduces the memory utilization.

### 1.3.19 Sentinel Server Might Shut Down When Running Searches That Span Across a Large Number Days

**Issue:** Sentinel server might shut down when you run searches that span across a large number of days. This is a sporadic issue. `(BUG 915845)`

**Fix:** Sentinel 7.3.1 improves memory utilization during searches that span across large number of days.

### 1.3.20 Selected ESS Type is Reset in Connector Editor Upon Closing ESS Editor

**Issue:** In Event Source Management, the Event Source Server (ESS) you select is reset in Connector Editor when you close the ESS Editor. `(BUG 896333)`

**Fix:** Sentinel 7.3.1 preserves the selected ESS after you close the ESS Editor.

### 1.3.21 Sentinel Web Interface Might Time Out Unexpectedly

**Issue:** Sentinel Web interface might time out unexpectedly and become unresponsive. (BUG 914121)

**Fix:** In Sentinel 7.3.1, the Web interface does not time out.

### 1.3.22 Solution Manager Does Not Deploy Imported Filters Created By Non-Admin Users

**Issue:** Solution Manager does not deploy filters when you create a solution pack using the filter created by a non-admin user, import the solution pack to another Sentinel system, and then try to deploy the filter. (BUG 910124)

**Fix:** You can deploy imported filters that are created by non-admin users. In the target Sentinel server, those filters will be owned by the admin user.

### 1.3.23 Sentinel Might Not Update Country Maps

**Issue:** Sentinel might display an error and become unresponsive while updating country maps. (BUG 908525)

**Fix:** Sentinel 7.3.1 modifies the maps update mechanism and fixes this issue.

### 1.3.24 Sentinel Does Not Display the Delta Information in Change Guardian Events If the Size is More Than 10 KB

**Issue:** Sentinel does not display the delta information in events sent by Change Guardian if the size of the delta information is more than 10 KB. (BUG 886894)

**Fix:** Sentinel 7.3.1 updates the delta information field in events so that it displays the content even if it is more than 10 KB size.

### 1.3.25 Sentinel Does Not Generate Reports If There are Commas in the Data Source Names

**Issue:** While generating distributed search reports, Sentinel displays an error if the data source names consist of commas. (BUG 871186)

**Fix:** Sentinel 7.3.1 generates reports in distributed environments correctly, even if there are commas in the data source names.

### 1.3.26 Sentinel Becomes Unresponsive When Generating Reports If the User Account That Scheduled the Report Does Not Exist

**Issue:** Reports generation takes a very long time to generate, and Sentinel becomes unresponsive if the user account that scheduled the report no longer exists. (BUG 886450)

**Fix:** When Sentinel deletes a user account, it also deletes all the report generation schedules created by that user account.

### 1.3.27 Synchronization Issues Between Sentinel and Sentinel Agent Manager

**Issues:**

- When you delete agents in Sentinel Agent Manager (SAM), the updates are not synchronized in Sentinel, and those agents might still display as active agents in Sentinel. (BUG 862431)
- Unmanaged agents and managed agents that are offline disappear from Sentinel after the daily agent scan, even though the same agents display correctly on SAM. Also, these agents send event data only for a short period of time after they disappear from Sentinel. (BUG 922073)
- Sentinel displays errors if there are uninstalled agents in SAM during SAM-Sentinel synchronization. (BUG 919624)
- Agent table synchronization takes a long time to complete, and prevents/delays data being written to the table. (BUG 927513)

**Fix:** Sentinel has a fine-tuned agents synchronization mechanism between Sentinel and Sentinel Agent Manager such that it updates only active agents.

### 1.3.28 Autocomplete Functionality in the Sentinel Login Page Might Cause Security Vulnerabilities

**Issue:** Autocomplete functionality in the Sentinel login page might cause security vulnerabilities, because it exposes user login credentials. (BUG 822435)

**Fix:** Sentinel 7.3.1 disables the autocomplete functionality.

### 1.3.29 Arrows Used for Sort Order in Event Sources Page are Almost Invisible

**Issue:** In the **Collection** > **Events Sources** page, the arrows that show the sorting order in Collector Managers, Event Source Servers, and Collector Plug-ins lists are not clearly visible. (BUG 897992)

**Fix:** In Sentinel 7.3.1, arrows that show the sorting order in event sources lists are clearly visible.

### 1.3.30 Sentinel Server Might Stop When Malformed Data is Sent To the Proxy Port

**Issue:** When the Sentinel proxy port receives malformed data such that the first 4 bytes of the data consumes large amounts of memory, Sentinel tries to allocate memory space for that data, and eventually runs out of memory. If this repeats for a few times, Sentinel server might shut down. (BUG 878690)

**Fix:** You can now configure the size of the data sent to the proxy port, the number of client connections, and the read timeout period. To configure these properties:

1. Log in as novell user and open the `/etc/opt/novell/sentinel/config/configuration.properties` file.
2. Set the `proxied.client.max.payload.size` property to the maximum data size for the proxy port.

   Default value is 1 GB. If the data exceeds the specified limit, Sentinel stops the data transfer.
3. Set the `proxied.client.max.connections` property to the maximum number of times a client can try to send data to the proxy port. Default value is 10.
4. Set the `proxied.client.read.timeout` property to the maximum time period after which the data transfer stops. Default value is 30 seconds.
5. Save the `configuration.properties` file and restart Sentinel.

Also, there is no limit on the data buffer size now. Sentinel buffers data dynamically while receiving data from the proxy port.

### 1.3.31 Errors When Processing Raw Data

**Issue:** Sentinel does not process raw data files that were not closed properly. This is a sporadic issue.(BUG 913841)

**Fix:** Sentinel correctly processes the raw data files that were not closed.

### 1.3.32 Sentinel Sometimes Displays an Error When Non-Administrators Run Reports

**Issue:** Sentinel might display an error when non-administrator users run reports that are created by the administrator user. (BUG 919966)

**Fix:** Non-administrator users can run and view all the reports to which their role has access permissions.

### 1.3.33 Cannot Add Data Sources or Authorized Requestors In Sentinel Appliance Installations

**Issue:** Sentinel displays an error when you try to add data sources or authorized requestors in Sentinel Appliance installations when two or more NICs are configured. (BUG 900177)

**Fix:** Perform the following steps after upgrading to Sentinel 7.3.1:

1. In the authorized requestor server, add the following property in the `/etc/opt/novell/sentinel/config/configuration.properties` file as follows:

   ```
   sentinel.distsearch.console.ip=<one of the authorized requestor's IP addresses>
   ```

2. In the data source server, add the following property in the `/etc/opt/novell/sentinel/config/configuration.properties` file as follows:

   ```
   sentinel.distsearch.target.ip=<one of the data source's IP addresses>
   ```

3. Restart Sentinel:

   ```
   rcsentinel restart
   ```

4. Log in to the authorized requestor server and click **Integration**. If the data source you want to add is already present, delete it and add it again using one of the IP addresses you specified in Step 2.

   Similarly, add authorized requestors using the IP addresses you specified in Step 1.

### 1.3.34 Sentinel Displays Irrelevant Data If the Event Search Criteria Contains Special Characters

**Issue:** Sentinel displays irrelevant event data if the event search criteria substring contains special characters such as `$` and `#` in event fields. (BUG 923724)

**Fix:** Perform the following steps to enable usage of special characters in event fields:

1. Log in as novell user and open the `etc/opt/novell/sentinel/config/configuration.properties` file.
2. Set the `indexedLog.tokenizedField.enableSplCharSrch` property to `true`.
3. Restart Sentinel.

### 1.3.35 Alert Dashboards Might Not Display Alerts in the Number of Alerts and Their Source Pane

**Issue:** Alert dashboards might not display any alerts in the **Number of Alerts and Their Source** pane, even though alerts are present. This happens because the default setting is to display alerts based on the longitude of their origin. `(BUG 924361)`

**Fix:** The **Number of Alerts and Their Source** pane now displays alerts based on the country of their origin by default.

### 1.3.36 Collector Manager Drops Events When Disconnected From Sentinel

**Issue:** While sending events to Sentinel, the Collector Manager drops events if it gets restarted or disconnected from Sentinel. `(BUG 916418)`

**Fix:** Collector Manager writes the events to a message broker while restarting or when disconnected from Sentinel, and sends these events to Sentinel when it re-establishes the connection.

### 1.3.37 Search Duration Fields are Overlapped By the Content of the Search Name Field

**Issue:** In the **Reports and Searches** page, the content of the search name field overwrites the search duration fields. This makes it difficult to view the search name correctly and also to select the search duration time range. `(BUG 928992)`

**Fix:** The search result label and the date range fields do not overlap now.

### 1.3.38 Map Updates Might Take a Long time

**Issue:** Map updates take a long time to complete and might also bring the Sentinel performance down if the maps are large in size. `(BUG 921905)`

**Fix:** Sentinel 7.3.1 improves memory utilization during large map updates.

### 1.3.39 Remote Collector Manager and Remote Correlation Engine Fail to Connect with Sentinel High Availability Server After a Failover

**Issue:** In Sentinel High Availability environments, remote Collector Manager and remote Correlation Engine fail to connect with Sentinel server after a failover. `(BUG 912476)`

**Fix:** Remote Collector Manager and remote Correlation Engine now connect with the Sentinel server after failover.

### 1.3.40 Alert Roll-up Fails When the Repeat Count Field is Configured to a Value in Alerts

**Issue:** When you create alerts through REST API, Sentinel creates new alerts instead of rolling up alert information to an existing alert when the **Repeat Count** field is configured to a value. `(BUG 909431)`

**Fix:** Sentinel ignores the **Repeat Count** field and rolls up alerts correctly.

### 1.3.41 Sentinel Might Delete Archived Partitions if it Cannot Access the Corresponding Online Partitions

**Issue:** Sentinel might delete archived partitions on the secondary storage if it cannot connect to the corresponding online partitions on primary storage. This is a sporadic issue. (BUG 927972)

**Fix:** Sentinel does not delete archived partitions on the secondary storage.

# 2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see the Technical Information for Sentinel page.

# 3 Upgrading to Sentinel 7.3.1

You can upgrade to Sentinel 7.3.1 from Sentinel 7.0 or later.

Download the Sentinel installer from the NetIQ Download website. For information about upgrading to Sentinel 7.3.1, see "Upgrading Sentinel" in the *NetIQ Sentinel Installation and Configuration Guide*.

## 3.1 Post Upgrade Configuration

After the upgrade, the Data Proxy User (formerly Search Proxy User) role will not have the **Allow users to manage alerts** permission. This permission is necessary for the role to be able to perform remote alert search. Assign the **Allow users to manage alerts** permission to the Data Proxy User role manually. For more information, see "Configuring Roles and Users" in the *NetIQ Sentinel Administration Guide*.

# 4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

The updates included in this service pack, including the Java 8 update and the security vulnerability fixes, might impact the following plug-ins:

- Cisco SDEE Connector
- SAP Connector
- Remedy Integrator

For any issues with these plug-ins, NetIQ will prioritize and fix the issues according to standard defect-handling policies. For more information about support polices, see Support Policies.

## 4.1 Cannot View Alerts with IPv6 Data in Alert Views

**Issue:** Sentinel alert views and alert dashboards do not display alerts that have IPv6 addresses in IP address fields. `(BUG 924874)`

**Workaround:** To view alerts with IPv6 addresses in Sentinel, perform the steps mentioned in NetIQ Knowledgebase Article 7016555.

## 4.2 Error When Configuring the NFS Storage After Upgrading Sentinel Appliance to Version 7.3.1

**Issue:** Sentinel displays an error when you try to configure NFS as secondary storage location after you Sentinel appliance to version 7.3.1. `(BUG 934851)`

**Workaround:** After upgrading to Sentinel appliance 7.3.1, restart the SLES operating system using the following command:

```
init 6
```

## 4.3 Exception in the Sentinel Server Log When You Upgrade Sentinel from Version 7.3 to Version 7.3.1

**Issue:** When you upgrade Sentinel from version 7.3 to version 7.3.1 and start the Sentinel server, you might see the following exception in the server log:

```
Invalid length of data object ......
```

`(BUG 933640)`

**Workaround:** Ignore the exception. There is no impact to Sentinel performance because of this exception.

## 4.4 Cannot Receive Events from Secure Configuration Manager After Upgrading to Sentinel 7.3.1

**Issue:** Sentinel uses the Diffie-Hellman protocol to communicate with Secure Configuration Manager. As part of fixing the Logjam vulnerability, the certificate key size for the Diffie-Hellman protocol in Sentinel has been increased to 2048. However, Secure Configuration Manager uses the default certificate key size; that is, 1024. Because of this mismatch, Secure Configuration Manager can no longer communicate with Sentinel. `(BUG 935987)`

**Workaround:** Until a fix is available from Secure Configuration Manager, you can perform the following steps:

---

**WARNING:** Performing this workaround overrides the fix for the Logjam vulnerability specified in Section 1.2, “Security Vulnerability Fixes,” on page 2.

---

1. Log in as novell user and open the `/etc/opt/novell/sentinel/config/configuration.properties` file.
2. Comment out the following line following line by prefixing `#`:

   ```
   jdk.tls.ephemeralDHKeySize=2048
   ```
3. Restart Sentinel.

## 4.5 Cannot Receive Events from Change Guardian After Upgrading to Sentinel 7.3.1

**Issue:** As part of fixing the Bar Mitzvah vulnerability, Sentinel disabled the RC4 ciphers on SSL ports enabled for the Web server. However, Change Guardian uses RC4 ciphers to communicate with Sentinel. Therefore, Change Guardian can no longer communicate with Sentinel. `(BUG 935401)`

**Workaround:** Until a fix is available from Change Guardian, you can perform the following steps:

---

**WARNING:** Performing this workaround overrides the fix for the Bar Mitzvah vulnerability specified in Section 1.2, “Security Vulnerability Fixes,” on page 2.

---

1. Log in as novell user and open the `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` file.
2. Delete the following lines from the ExcludeCipherSuites list:

   ```
   <Item>SSL_RSA_WITH_RC4_128_SHA</Item>
   <Item>SSL_RSA_WITH_RC4_128_MD5</Item>
   ```

3 Restart Sentinel.

4 Restart the Change Guardian service in the Change Guardian agent computer.

## 4.6 When Integrated with Change Guardian 4.1, Sentinel Does Not Display Change Guardian Delta Attached Information

**Issue:** When Sentinel is integrated with Change Guardian 4.1, it does not display Change Guardian delta attached information, in spite of being configured to receive Change Guardian events. `(BUG 936704)`

**Workaround:** Upgrade Change Guardian to version 4.1.1 or later.

Or

The Change Guardian Solution Pack 2011.1r4 resolves this issue. Until it is officially released, you can download the Solution Pack from the Sentinel Plug-ins Previews website. You can view the delta information in the following Change Guardian reports after you apply the Solution Pack:

- Change Guardian Events
- Change Guardian Events by Asset
- Change Guardian Events by Policy
- Change Guardian Events by User

## 4.7 Bar Mitzvah Security Vulnerability in Sentinel Link Connector

**Issue:** The Bar Mitzvah security vulnerability exists in Sentinel Link Connector. Sentinel Link Connector uses the RC4 algorithm in SSL and TSL protocols, which might allow plaintext recovery attacks against the initial bytes of a stream. For more information, see CVE-2015-2808. `(BUG 933741)`

**Workaround:** The Sentinel Link Connector version 2011.1r4 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

## 4.8 Issue with Sentinel Appliance Login

**Issue:** If you specified a $ character in the password, Sentinel stores the password differently in the database depending on where the $ is placed in the password. If the password starts with the $ special character, Sentinel stores the password with a file name. If the $ character is somewhere in the middle of the password, Sentinel truncates the password to the location of the $ character. `(BUG 734500)`

**Workaround:** The actual password is stored in the `home/novell/.pgpass` file. Obtain the password from this file and then log in to Sentinel. For example, if you specified the password as abc$123, the Sentinel stores the password as abc in the `.pgpass` file. You can log in to Sentinel by specifying abc as the password.

## 4.9 The Agent Manager Connector Does Not Set the Connection Mode Property in Events If the Associated Collector Supports Multiple Connection Modes

**Issue:** The Agent Manager Connector version 2011.1r3 does not set the CONNECTION_MODE property in the events if the Collector parsing the events supports multiple connection modes. (BUG 880564)

**Workaround:** The Agent Manager Connector version 2011.1r5 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

## 4.10 Security Vulnerability in SSL 3.0

**Issue:** A vulnerability exists in SSL 3.0 that might allow plaintext of secure connections to be calculated. For more information, see CVE-2014-3566. This vulnerability exists in the bundled version of Syslog Connector 2011.1r4 since it uses the SSL protocol. (BUG 920018)

**Workaround:** The Syslog Connector version 2011.1r5 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

## 4.11 Sentinel Agent Manager Does Not Consider the RawDataTapFileSize Configuration

**Issue:** Sentinel Agent Manager ignores the value specified in `RawDataTapFileSize` attribute in the `SMServiceHost.exe.config` file for the raw data file size configuration, and stops writing to the raw data file when the file size reaches 10 MB. (BUG 867954)

**Workaround:** Manually copy the content of the raw data file into another file and clear it when the file size reaches 10 MB, so that Sentinel Agent Manager can write new data into it.

## 4.12 Tips Table Search Does Not Return the Complete List of Alert Fields in Upgraded Sentinel Installations

**Issue:** In upgraded installations of Sentinel 7.3, when you search for alert attributes in the Tips table in the Web interface, the search does not return the complete list of alert fields. However, alert fields display correctly in the Tips table if you clear the search. (BUG 914755)

**Workaround:** There is no workaround at this time.

## 4.13 Data Synchronization Fails While Synchronizing IPv6 Addresses in Human Readable Format

**Issue:** Data synchronization fails when you try to synchronize IPv6 address fields in a human readable format to external databases. For information about configuring Sentinel to populate the IP address fields in human readable dot notation format, see "Creating a Data Synchronization Policy" in the *NetIQ Sentinel Administration Guide*. (BUG 913014)

**Workaround:** To fix this issue, manually change the maximum size of the IP address fields to at least 46 characters in the target database, and re-synchronize the database.

## 4.14 Event Search Does Not Respond if You Do Not Have Any Event Viewing Permissions

**Issue:** If run an event search when your role's security filter is blank and your role does not have event viewing permissions, the search does not complete. The search does not display any error message about the invalid event viewing permissions. (BUG 908666)

**Workaround:** Update the role with one of the following options:

1. Specify a criteria in the **Only events matching the criteria** field. If users in the role should not see any events, you can enter **NOT sev:[0 TO 5]**.
2. Select **View system events**.
3. Select **View all event data (including raw data and NetFlow data)**.

## 4.15 The Event fields Panel is Missing in the Schedule Page When Editing Some Saved Searches

**Issue:** When editing a saved search upgraded from Sentinel 7.2 to a later version, the **Event fields** panel, used to specify output fields in the search report CSV, is missing in the schedule page. (BUG 900293)

**Workaround:** After upgrading Sentinel, recreate and reschedule the search to view the **Event fields** panel in the schedule page.

## 4.16 Sentinel Does Not Return Any Correlated Events When You Search for Events for the Deployed Rule with the Default Fire Count Search

**Issue:** Sentinel does not return any correlated events when you search for all correlated events that were generated after the rule was deployed or enabled, by clicking the icon next to **Fire count** in the **Activity statistics** panel in the Correlation Summary page for the rule. (BUG 912820)

**Workaround:** Change the value in the **From** field in the Event Search page to a time earlier than the populated time in the field and click **Search** again.

## 4.17 Sentinel in FIPS 140-2 Mode Does Not Display Change Guardian Delta Attached Information

**Issue:** Sentinel running in FIPS 140-2 mode does not display Change Guardian delta attached information when you search for Change Guardian events and click the **Change Guardian** icon, in spite of being configured to receive Change Guardian events. Change Guardian 4.1.1.1 and earlier versions do not support sending events in FIPS 140-2-compatible mode. (BUG 912230)

**Workaround:** There is no workaround at this time.

## 4.18 Data Collection and Data Synchronization With the DB2 Database Fail After Upgrading to Sentinel 7.3

**Issue:** Upgrading to Sentinel 7.3 causes data collection and data synchronization with the DB2 database to fail, because the upgrade removes the IBM DB2 JDBC driver. (BUG 909343)

**Workaround:** After upgrading to Sentinel 7.3, add the correct JDBC Driver and configure it for data collection and data synchronization, by performing the following steps:

1. Copy the correct version of the IBM DB2 JDBC driver (`db2jcc-*.jar`) for your version of the DB2 database in the `/opt/novell/sentinel/lib` folder.
2. Ensure that you set the necessary ownership and permissions for the driver file.
3. Configure this driver for data collection. For more information, see the Database Connector documentation.

## 4.19 New Incoming Alerts Incorrectly Appear to be Selected When You Modify Existing Alerts

**Issue:** When you click **Select All** in alerts views to select alerts, deselect few alerts, and modify them, new incoming alerts are also selected in the refreshed alert views. This results in wrong count of alerts selected for modification, and also it appears as if you are modifying new incoming alerts too. However, only the originally selected alerts are modified. `(BUG 904830)`

**Workaround:** No new alerts will appear in the alert view if you create the alert view with a custom time range.

## 4.20 Loading Historical Security Intelligence Data Takes a Long Time

**Issue:** Historical Security Intelligence (SI) data takes a long time to load in Sentinel systems that have a high Events Per Second (EPS) load. `(BUG 908599)`

**Workaround:** If you are creating a security intelligence dashboard with historical data, plan to deploy the dashboard when the load on your system is lower, if possible. There is no other workaround at this time.

## 4.21 Security Intelligence Dashboard Displays Invalid Baseline Duration When Regenerating a Baseline

**Issue:** During Security Intelligence baseline regeneration, the start and finish dates for the baseline are incorrect and display 1/1/1970. `(BUG 912009)`

**Workaround:** The correct dates are updated after the baseline regeneration is complete.

## 4.22 Sentinel Server Shuts Down When Running a Search If There Are Large Number of Events in a Single Partition

**Issue:** Sentinel server shuts down when you run a search if there are a large number of events indexed in a single partition. `(BUG 913599)`

**Workaround:** Create retention policies in such a way that there are at least two partitions open in a day. Having more than one partition open helps reduce the number of events indexed in partitions.

You can create retention policies that filter events based on the `estzhour` field, which tracks the hour of the day. Therefore, you can create one retention policy with `estzhour:[0 TO 11]` as the filter and another retention policy with `estzhour:[12 TO 23]` as the filter.

For more information, see "Configuring Data Retention Policies" in the *NetIQ Sentinel Administration Guide*.

## 4.23 Error While Using the report_dev_setup.sh Script to Configure Sentinel Ports for Firewall Exceptions on Upgraded Sentinel Appliance Installations

**Issue:** Sentinel displays an error when you use the `report_dev_setup.sh` script to configure Sentinel ports for firewall exceptions. `(BUG 914874)`

**Workaround:** Configure Sentinel ports for firewall exceptions through the following steps:

1. Open the `/etc/sysconfig/SuSEfirewall2` file.
2. Change the following line:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   to

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Restart Sentinel.

## 4.24 Sentinel Generic Collector Performance Degrades When Generic Hostname Resolution Service Collector is Enabled

**Issue:** Sentinel Generic Collector performance degrades when Generic Hostname Resolution Service Collector is enabled on Microsoft Active Directory and Windows Collector. EPS decreases by 50% when remote Collector Managers send events. `(BUG 906715)`

**Workaround:** There is no workaround at this time.

## 4.25 Sentinel Cannot Access Security Intelligence, Netflow, and Alert Data in FIPS 140-2 Mode

**Issue:** When you install Sentinel in FIPS 140-2 mode, connector to Security Intelligence database fails to start, and Sentinel cannot access Security Intelligence, Netflow, and alert data. `(BUG 915241)`

**Workaround:** Restart Sentinel after installing and configuring in FIPS 140-2 mode.

## 4.26 Security Intelligence Database and Alert Dashboard Occasionally Do Not Work in Upgraded Custom Installations of FIPS 140-2 Enabled Sentinel

**Issue:** When you upgrade to Sentinel 7.3 from a custom installation of Sentinel that was installed by a non-root user and was configured in FIPS 140-2 mode, Security Intelligence database and Alert Dashboard occasionally do not start. `(BUG 916285)`

**Workaround:** Perform the following steps:

1. Go to `<`*`custom installation directory`*`>/opt/novell/sentinel/bin` to know the Sentinel Indexing Service.
2. Run the following command:

   ```
   ./si_db.sh status
   ```

   Verify whether the following output displayed:

```
Connection between alert store and indexing service is running.
Security Intelligence database is running.
Indexing service is running.
```

If any of the above mentioned three services are not running, perform the following steps.

3. Run the following command to stop Sentinel:

   `rcsentinel stop`

4. Log in to the Sentinel server as the novell user.

5. Run the following command:

   `<custom installation directory>/opt/novell/sentinel/bin/si_db.sh startnoauth`

6. Run the following commands to add dbauser and appuser users:

   `cd <custom installation directory>/opt/novell/sentinel/3rdparty/mongodb/bin`

   `./mongo`

   `use admin`

   `db.addUser ("dbauser", "novell")`

   `use analytics`

   `db.addUser ("appuser", "novell")`

   `exit`

7. Stop the MongoDB database:

   `<custom installation directory>/opt/novell/sentinel/bin/si_db.sh stop`

8. Perform the following steps to add encrypted password fields:

   **8a** Run the following command to get the encrypted password for the novell user:

   `<custom installation directory>/opt/novell/sentinel/bin/encryptpwd -e novell`

   Encrypted password is displayed. For example:

   `bVWOzu6okMmMCkgM0aHeQ==`

   **8b** In the `configuration.properties` file, update the `baselining.sidb.password` and `baselining.sidb.dbpassword` properties with the encrypted

   password. for example:

   `baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==`

   `baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==`

9. Exit from novell user account and start Sentinel as root user using the following command:

   `rcsentinel start`

---

**NOTE:** Run the `configure.sh` script to reset the password whenever needed. For more information about running the `configure.sh` script, see “Modifying the Configuration after Installation” in the *NetIQ Sentinel Installation and Configuration Guide*.

---

## 4.27 Sentinel Does Not Configure the Sentinel Appliance Network Interface By Default

**Issue:** When installing Sentinel Appliance, the network interface is not configured by default. `(BUG 867013)`

**Workaround:** To configure the network Interface:

1. In the Network Configuration page, click **Network Interfaces**.
2. Select the network interface and click **Edit**.
3. Select **Dynamic Address** and then select either **DHCP** or **Static assigned IP Address**.
4. Click **Next** and then **OK**.

## 4.28 The Web Browser Displays an Error When Exporting Search Results in Sentinel

**Issue:** When exporting search results in Sentinel, the Web browser might display an error if you modify the operating system language settings. `(BUG 834874)`

**Workaround:** To export search results properly, perform either of the following:

- While exporting the search results, remove any special characters (outside the ASCII characters) from the export filename.
- Enable UTF-8 in the operating system language settings, restart the machine, and then restart the Sentinel server.

## 4.29 Partitions Removed from Secondary Storage are Also Removed from Primary Storage

**Issue:** If the number of days of data that secondary storage can hold is less than the number of days of data that primary storage holds, Sentinel does not use the disk space in primary storage efficiently. Partitions removed from secondary storage to free up space will also be removed from primary storage. `(BUG 860888)`

**Workaround:** Allocate enough space in secondary storage to hold data for the total number of days you want to keep online (searchable).

For more information, see "Event Data" in the *NetIQ Sentinel Administration Guide*.

## 4.30 Sentinel Services Might Not Start Automatically After the Installation

**Issue:** On systems with more than 2 TB disk space, Sentinel might not start automatically after the installation. `(BUG 846296)`

**Workaround:** As a one-time activity, start the Sentinel services manually by specifying the following command:

```
rcsentinel start
```

## 4.31 Cannot Enable Kerberos Authentication in Sentinel Appliance Installations

**Issue:** In Sentinel appliance installations, if you configure Kerberos authentication in the Kerberos module, the console displays a confirmation message that the Kerberos client configuration was successful. When you view the Kerberos module again, however, the **Enable Kerberos Authentication** option is deselected. `(BUG 843623)`

**Workaround:** There is no workaround at this time.

## 4.32 Unable to Install the Remote Collector Manager If the Password Contains Special Characters

**Issue:** When you install a remote Collector Manager, if you specify a password that contains special characters, such as '$', '"', '\', or '/', the installation fails with errors. `(BUG 812111)`

**Workaround:** Do not use special characters in the remote Collector Manager password.

## 4.33 Restarting a Remote Collector Manager Causes Some Event Sources to Lose Connection

**Issue:** When you restart a remote Collector Manager appliance, the Syslog event sources connected on the UDP port lose connection. `(BUG 795057)`

**Workaround:** There is no workaround available at this time.

## 4.34 Unable to View More Than One Report Result at a Time

**Issue:** While you wait for one report result PDF to open, particularly report results of 1 million events, if you click another report result PDF to view, the report result is not displayed. `(BUG 804683)`

**Workaround:** Click the second report result PDF again to view the report result.

## 4.35 Agent Manager Requires SQL Authentication When FIPS 140-2 Mode is Enabled

**Issue:** When FIPS 140-2 mode is enabled in your Sentinel environment, using Windows authentication for Agent Manager causes synchronization with the Agent Manager database to fail. `(BUG 814452)`

**Workaround:** Use SQL authentication for Agent Manager when FIPS 140-2 mode is enabled in your Sentinel environment.

## 4.36 Sentinel High Availability Installation in FIPS 140-2 Mode Displays an Error

**Issue:** If FIPS 140-2 mode is enabled, the Sentinel High Availability installation displays the following error:

```
Sentinel server configuration.properties file is not correct. Check the
configuration file and then run the convert_to_fips.sh script again to enable FIPS
mode in Sentinel server.
```

However, the installation completes successfully. `(BUG 817828)`

**Workaround:** There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in FIPS 140-2 mode.

## 4.37 Sentinel High Availability Installation in Non-FIPS 140-2 Mode Displays an Error

**Issue:** The Sentinel High Availability installation in non-FIPS 140-2 mode completes successfully but displays the following error twice:

`/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments`

`(BUG 810764)`

**Workaround:** There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in non-FIPS 140-2 mode.

## 4.38 Appliance Update From Versions Prior to Sentinel 7.2 Fails in WebYaST

**Issue:** Appliance update from versions prior to Sentinel 7.2 fails because the vendor for the update packages has changed from Novell to NetIQ. `(BUG 780969)`

**Workaround:** Use the zypper command to upgrade the appliance. For more information, see "Upgrading the Appliance by Using zypper" in the *NetIQ Sentinel Installation and Configuration Guide*.

## 4.39 Error While Installing Correlation Rules

**Issue:** Solution Manager does not install correlation rules when a correlation rule with an identical name already exists on the system. A `NullPointerException` error is logged in the console. `(BUG 713962)`

**Workaround:** Ensure that all correlation rules have a unique name.

## 4.40 Sentinel Link Action Displays Incorrect Message

**Issue:** When you execute a Sentinel Link action from the Web interface Sentinel displays a success message even though the Sentinel Link Connector integrator test failed from the Sentinel Control Center. `(BUG 710305)`

**Workaround:** There is no workaround at this time.

## 4.41 Dashboard and Anomaly Definitions with Identical Names

**Issue:** When a Security Intelligence dashboard and an anomaly definition have identical names, the dashboard link is disabled on the Anomaly Details page. `(BUG 715986)`

**Workaround:** Ensure you use unique names when creating dashboards and anomaly definitions.

## 4.42 Active Search Jobs Duration and Accessed Columns Inaccuracies

**Issue:** The Sentinel Web interface displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Web interface computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Web interface clock is set to 1:30 PM and the Sentinel server clock is set to 2:30 PM. `(BUG 719875)`

**Workaround:** Ensure the time on the computer you use to access the Sentinel Web interface is the same as or later than the time on the Sentinel server computer.

## 4.43 IssueSAMLToken Audit Event Displays Incorrect Information in the Security Intelligence Dashboard

**Issue:** When you log in to the security dashboard and perform a search for `IssueSAMLToken` audit event, the `IssueSAMLToken` audit event displays incorrect hostname (InitiatorUserName) or (IP address) SourceIP. `(BUG 870609)`

**Workaround:** There is no workaround at this time.

## 4.44 Sentinel Control Center Does Not Launch When NetIQ Identity Manager Designer is Installed on the Client Computer

**Issue:** Sentinel Control Center does not launch when the NetIQ Identity Manager Designer is installed on the client computer and Designer uses the system JRE. Designer needs to add some supporting jar files like `xml-apis.jar` to the `lib/endorsed` directory. Some of the classes in the `xml-apis.jar` file override the corresponding classes in the system JRE that is used by the Sentinel Control Center. `(BUG 888085)`

**Workaround:** Configure Designer to use its own JRE.

## 4.45 Sentinel Agent Manager Does Not Capture the Windows Insertion String Fields With Null Values

**Issue:** While collecting event data, Sentinel Agent Manager does not capture the Windows Insertion String fields with null values. `(BUG 838825)`

**Workaround:** There is no workaround at this time.

# 5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

# 6 Legal Notice